REMARKS

The application included claims 1, 2, 4-12, 14-20, 22, and 24-34 prior to entering this amendment.

Claims 7, 17, and 27 are indicated as containing allowable material.

The Applicant amends claims 1, 5, 10-12, 14-16, 18-20, 24-26, 28, 30, 31, and 33, and cancels claims 7 and 29 without prejudice.

The Applicant adds new claims 36-38. No new matter is added.

The application remains with claims 1, 2, 4-6, 8-12, 14-20, 22, 24-28, 30-34, and 36-38 after entering this amendment.

APPLICANT'S COMMENTS ON EXAMINER'S STATEMENT OF ALLOWABLE SUBJECT MATTER

Applicant acknowledges Examiner's statement of allowable subject matter of claims 7, 17, and 27 and agrees that the claimed subject matter is patentable. However, Applicant takes no position regarding the statement of allowable subject matter presented by the Examiner other than the positions Applicant may have previously taken during prosecution. Therefore, the Examiner's statement of allowable subject matter should not be attributed to Applicant as an indication of the basis for Applicant's belief that the claims are patentable. Furthermore, Applicant respectfully asserts that there may also be additional reasons for patentability of the claimed subject matter not explicitly stated in this record and Applicant does not waive its rights to such arguments by not further addressing such reasons herein.

Applicant rewrites claim 7 in independent form as new claim 38, and cancels claim 7. While Applicant agrees with the Examiner that claims 17 and 27 are allowable, Applicant respectfully declines to amend claims 17 and 27 on the basis that the independent claims 11 and 31, upon which they depend, are themselves allowable as discussed below with respect to the 35 U.S.C. § 103 rejection.

Claim Rejections - 35 U.S.C. § 103

The Examiner rejected claims 1, 2, 4-6, 8-12, 14-16, 18-20, 22, 24-26, and 28-34 under 35 U.S.C. § 103(a) over Cowie *et al.* (U.S. Patent Application Publication No. 2003/0023865), and variously in view of Atkinson (U.S. Patent 5,892,904), Richer (SANS/GIAC Practical

Assignment for GSEC Certification Version 1.4b: Steganalysis: Detecting hidden information with computer forensic analysis, SANS Institute 2003), and Charbonneau (U.S. Patent 7,526,654).

Whereas the rejection is traversed, Applicant amends claims 1, 5, 10-12, 14-16, 18-20, 24-26, 28, 30, 31, and 33, and cancels claims 7 and 29 in order to expedite prosecution, and without prejudice to pursuing the claims as previously presented or in other forms in a continuation or other application. For example, claim 1 recites a method, comprising:

> locating a steganographic program comprising executable code that includes both read and write software calls;
>
> obtaining a steganographic signature by reading a partial section of the executable code, wherein the steganographic program is configured to introduce steganographic items into a computer file via the software calls;
>
> identifying computer files comprising software code;
>
> obtaining one or more test signatures by reading partial sections of the software code;
>
> comparing the steganographic signature with the one or more test signatures; and
>
> displaying a listing of which of the computer files comprise the test signatures that provide a match with the steganographic signature.

Cowie is directed to a system of detecting computer programs where fingerprint data indicative of predetermined characteristics of resource data are used to compare the suspect file with the library of Trojans and worms (paragraph 0012). In rejecting claim 1, the Examiner acknowledged that Cowie fails to disclose obtaining a steganographic signature by reading a partial section of the executable code, and instead suggested that the features are disclosed by the newly cited reference to Atkinson. Applicant respectfully disagrees.

Atkinson is directed to a method of certifying or signing an executable file transmitted over a network (col. 2, lines 33-40). According to Atkinson, the executable file or its header is searched for a publisher signature 110 in the form of a cryptographic message (col. 7, lines 35-42). The user is then notified when the published signature 110 is invalid, so that the file may not be opened or run (col. 7, line 64 to col. 8, line 2).

Even assuming, for argument's sake, that Atkinson's publisher signature included in an executable file discloses a partial section of the executable code, Applicant respectfully submits that the combination of Cowie with the Atkinson reference nevertheless still fails to disclose *obtaining a steganographic signature by reading a partial section of the executable code*, as

recited by claim 1. At page 3 of the Office Action, the Examiner suggested that it would be obvious to combine Cowie with Atkinson since this would increase the probability of detecting hidden malware in a file. Applicant respectfully disagrees.

Cowie teaches away from reading any executable code by describing that in order to read the code of the packed files, one would have to decompress the files (paragraphs 0005). On the other hand, Cowie discloses that his data indicia are identified without decompressing the files (paragraph 00012). The proposed combination of Cowie with Atkinson would therefore require Cowie's system to first decompress the file so that Atkinson's publisher signature 110 could be read. However, this would be contrary to the teachings of Cowie, as described above.

The Supreme Court acknowledged the importance of identifying "a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does" in an obviousness determination. *KSR*, 127 S. Ct. 1727 at 1731 (2007). Additionally, if one of the references 'teaches away' from the combination of references (i.e., teaches away from the missing claim element), it is strong evidence of non-obviousness.

Applicant respectfully submits that since Atkinson's publisher signature 110 is directed to the purpose of authenticating the sender of the file rather than Cowie's stated purpose of detecting trojans or worms, and furthermore since Cowie teaches away from such a proposed combination, it would not have been obvious to combine these references in the proposed manner without the use of impermissible hindsight. Rather, the disparate purposes of Cowie and Atkinson could both be accomplished separately even if a system had been developed that took into account both of the references. That is to say, a header of the file could be analyzed according to Cowie to check for worms and viruses, whereas the file could be checked according to Atkinson to determine if there is a valid publisher signature.

Claim 1 is amended to recite additional features which serve to distinguish the cited references. For example, claim 1 recites *locating a steganographic program comprising executable code that includes both read and write software calls*, *identifying computer files comprising software code*, *obtaining one or more test signatures by reading partial sections of the software code*, and *comparing the steganographic signature with the one or more test signatures*. As acknowledged by the Examiner, Cowie fails to disclose a steganographic program in the first instance. Atkinson also fails to disclose a steganographic program.

The Examiner cited Richer to disclose the general concept of steganalysis. Richer provides an overview of steganography, including a brief review of a number of steganographic tools (pages 6-9 of Richer). The different tools are described variously as an evaluation of hash values of suspected files, compressibility of the suspected files, analysis of an image for embedded data, etc. Applicant notes that neither the "original file MD5 hash" nor the "MD5 hash of a suspect file" as identified by the Examiner (page 3 of the Office Action) are obtained by reading executable code of a steganographic program. The description of the tools in Richer also fails to disclose the various other features recited by amended claim 1, and accordingly Richer fails to cure the deficiencies of Cowie and Atkinson described above.

Claims 11 and 31 are believed to be allowable over the cited art for similar reasons as claim 1. As claims 2, 4-6, 8-10, 12, 14-16, 18-20, 22, 24-26, 28, 30, and 32-34 depend directly or indirectly from independent claims 1, 11, or 31, the comments and revisions directed above to claims 1, 11, or 31 apply equally to claims 2, 4-6, 8-10, 12, 14-16, 18-20, 22, 24-26, 28, 30, and 32-34, respectively. In addition, claims 2, 4-6, 8-10, 12, 14-16, 18-20, 22, 24-26, 28, 30, and 32-34 recite further subject matter. Accordingly, reconsideration and withdrawal of the rejection of claims 1, 2, 4-6, 8-12, 14-16, 18-20, 22, 24-26, 28, and 30-34 is respectfully requested.

Any statements made by the Examiner that are not addressed by the Applicant do not necessarily constitute agreement by the Applicant. In some cases, the Applicant may have amended or argued the independent claims thereby obviating grounds for rejection of the dependent claims.

New Claims

The Applicant adds new claims 36-38 for consideration. No new matter is added.

CONCLUSION

For the foregoing reasons, the Applicant respectfully requests reconsideration and allowance of the present application. The Examiner is encouraged to telephone the undersigned at (503) 546-1812 if it appears that an interview would be helpful in advancing the case.

Customer No. 73552

Respectfully submitted,

STOLOWITZ FORD COWGER LLP

Bryan Kirkpatrick

Bryan D. Kirkpatrick
Reg. No. 53,135

STOLOWITZ FORD COWGER LLP
621 SW Morrison Street, Suite 600
Portland, OR 97205
(503) 224-2170